AO 106 (Rev. 06/09) Application for a Search Warrant

FILED

UNITED STATES DISTRICT COURT

NOV 16 2020

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
MICROSOFT SURFACE PRO LAPTOP S/N 002181271557 CURRENTLY LOCATED AT THE ATF TULSA FIELD OFFICE EVIDENCE VAULT (ATF EXH 000022)

Case No. 20-MJ-434-PJC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922(g)(1)	**Felon in Possession of Firearm**
18 U.S.C. § 922(g)(2)	**Fugitive From Justice in Possession of Firearm**
21 U.S.C. § 846	**Drug Conspiracy**
21 U.S.C. § 841(a)(1)	**Possession of Controlled Substance with Intent to Distribute**
18 U.S.C. § 1344	**Bank Fraud**
18 U.S.C. § 513	**Utter Forged or Counterfeit Security**
18 U.S.C. § 1028	**Identity Theft**
18 U.S.C. § 1028A	**Aggravated Identity Theft**

The application is based on these facts:

See Affidavit of Ashley Stephens, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Ashley Stephens, ATF
Printed name and title

Sworn to before me and signed in my presence.

by telephone

Date: 11/16/20

Judge's signature

City and state: Tulsa, OK

Frank H. McCarthy, U.S. Magistrate
Printed name and title

Paul J. Cleary
U.S. Magistrate Judge
333 W. 4th Street
Room 3355 U.S. Courthouse
Tulsa, OK 74103

IN THE UNITED STATES DISTRICT COURT FOR THE

NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF MICROSOFT SURFACE PRO LAPTOP S/N 002181271557 CURRENTLY LOCATED AT THE ATF TULSA FIELD OFFICE EVIDENCE VAULT (ATF EXH 000022)	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Ashley Stephens, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). I have been so employed since July of 2004. Before joining the ATF, I was employed as a Police Officer with the Tahlequah Police Department, in Tahlequah, Oklahoma, for three years. I successfully completed the Council on Law Enforcement Education and Training Academy as required by the State of Oklahoma for peace officer certification. I also completed the Criminal Investigator Training Program required by the ATF to be an ATF criminal investigator. I also completed the Special Agent Basic Training Academy required by ATF for all special agents employed by ATF. In connection with my official duties as an ATF Special Agent,

I investigate criminal violations of Federal Firearms Laws, Federal Arson Laws, Federal Explosives Laws and Federal Narcotics laws.

3. I hold a Bachelor's of Science Degree in Criminal Justice from Northeastern State University and I also have a Master's of Forensic Science Degree from Oklahoma State University.

4. During the first four (4) years of my employment with ATF, I was assigned to the North Texas High Intensity Drug Trafficking Area (HIDTA) Violent Crime Task Force where I was responsible for investigating criminal violations of Federal Firearms Laws and the Controlled Substances Act. I was the lead case agent for an Organized Crime Drug Enforcement Task Force (OCDETF) which resulted in numerous drug and firearm seizures. I have been the affiant for numerous state and federal search warrants. I have been involved in multiple investigations over my career which have resulted in the seizure of controlled substances and firearms, resulting in the successful prosecution of individuals involved. During my career, I have received hundreds of hours of training, including training regarding the investigation of those who are involved in the armed illicit distribution of controlled substances and training regarding individuals who commit fraudulent acts. I have received training and have experience including, but not limited to, working in an undercover capacity, surveillance, management of confidential informants, drug-trafficking conspiracies, money laundering, organized criminal activity investigations, the preparation and execution of firearm and drug related search warrants and debriefing of informants and witnesses.

5. I am an ATF Certified Explosives Specialist (Certification Number 12-42) and as such have received numerous hours of training regarding explosives and the investigation of explosive cases. I have attended numerous explosive schools i.e. Certified Explosive Specialist Basic, Advanced Explosives Disposal Techniques, Chemistry of Pyrotechnics, Homemade

Explosives Identify Process and Disposal, and Naval Basic Improvised Explosive Devices to name a few. I am also well versed in the Federal firearms laws.

6. I have received and completed the Firearms Interstate Nexus Training Basic School, provided by the ATF Firearms Technology Branch in Martinsburg, WV. During the training at the Firearms Interstate Nexus Training Course in Martinsburg, WV, I personally examined the ATF Firearms Technology Branch's Reference Collection, which includes approximately 10,000 firearms. In the course of my duties in establishing firearms interstate commerce, I have consulted various firearm publications and periodicals, have accessed official licensing files and have examined other documents. I have also consulted with other firearms experts, all of which leads to my expertise in the movement of firearms in interstate commerce. As an expert I have testified in federal court regarding interstate nexus and firearms' subsequent effect on and travel status of firearms as they pertain to interstate commerce.

7. I am also a Certified Fire Investigator responsible for providing technical support and analysis to assist other ATF Special Agents in fire investigations and training activities. This technical support includes: fire origin and cause determinations, court preparation and presentation of evidence, technical interpretation of fire-related information, and presentation of expert witness opinions.

8. As a result of my training and experience as an ATF Special Agent, I am familiar with Federal crime laws and know it is a violation of Title 18 United States Code Section 922(g)(1) for any person convicted of a felony to possess a firearm or ammunition that has traveled in or affected interstate or foreign commerce. I also know that it is a violation of Title 18 United States Code Section 922(g)(2) for any person who is a fugitive from justice to possess a firearm or ammunition that has traveled in or affected interstate or foreign commerce. Furthermore it is also

a violation of Title 21 United States Code Section 841(a)(1) for any person to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance. It is a violation of Title United States Code Section 846 for any person to attempt or conspire to commit the crime of distribution of controlled substances. Additionally, I know that it is a violation of Title 18, United States Code, Section 513 to utter a forged or counterfeit security. It is also a crime against the United States commit bank fraud in violation of Title 18, United States Code, Section 1344. I also know that it is a violation of Title 18, United States Code, Section 1028 to commit crimes of identity theft and a violation of Title 18, United States Code, Section 1028A to commit aggravated identity theft. It is also a violation of Title 18, United States Code, Section 1343 to commit wire fraud. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

9. The property to be searched is a Microsoft Surface Pro Laptop, serial number 002181271557 hereinafter the "Device." The Device is currently located inside the evidence vault of the Bureau of Alcohol, Tobacco Firearms and Explosives Tulsa Field Office located at 125 W 15th Suite 600, Tulsa within the Northern District of Oklahoma.

10. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

11. On October 30th, 2020, ATF Agents were notified by the United States Marshal Service that they were searching for an outstanding fugitive from the State of Kansas, named Sean Bonham WINDSOR. WINDSOR was also wanted in reference to two shootings that had

occurred in the Wichita, KS area. USMS Deputies had received information that WINDSOR was currently at a residence located at 3510 E 143rd Place South, Bixby, Oklahoma.

12. I, along with, Special Agent Carlos Sandoval and Resident Agent in Charge Justin Demaree had been to the residence on the day prior in reference to separate case and had made contact with the lessee of residence, Ms. Taylor SHARKEY. Due to mine and RAC Demaree's recent contact with Ms. Sharkey, the decision was made to call Ms. Sharkey and utilize a ruse to get her out of the house and to be able to ascertain if WINDSOR was in fact inside the residence. WINDSOR's criminal history was extensive and due to the circumstances involving the shootings, agents felt this to be the safest plan possible.

13. USMS Deputies were set up in the area where they had a good view of the aforementioned residence and were conducting real-time surveillance. RAC Demaree made a call to SHARKEY. SHARKEY indicated that she was not currently home, but would return home at around 11:15 am. It was shortly after this call, that USMS Deputies observed an individual, who matched WINDSOR's description come from around the residence. The individual walked away from the residence and entered a nearby port-a-potty. The individual exited the port-a-potty and USMS Deputies confirmed that the individual was in fact WINDSOR. WINDSOR was taken into custody without incident. Two cellular telephones, a black Samsung touch screen model SM-5102DL(GP) having an IMEI # of 356327115106970 and a black Samsung touch screen which has a gold sticker on the back (Exact model and IMEI could be determined without accessing this particular phone) were seized from WINDSOR's pockets during a search incident to arrest.

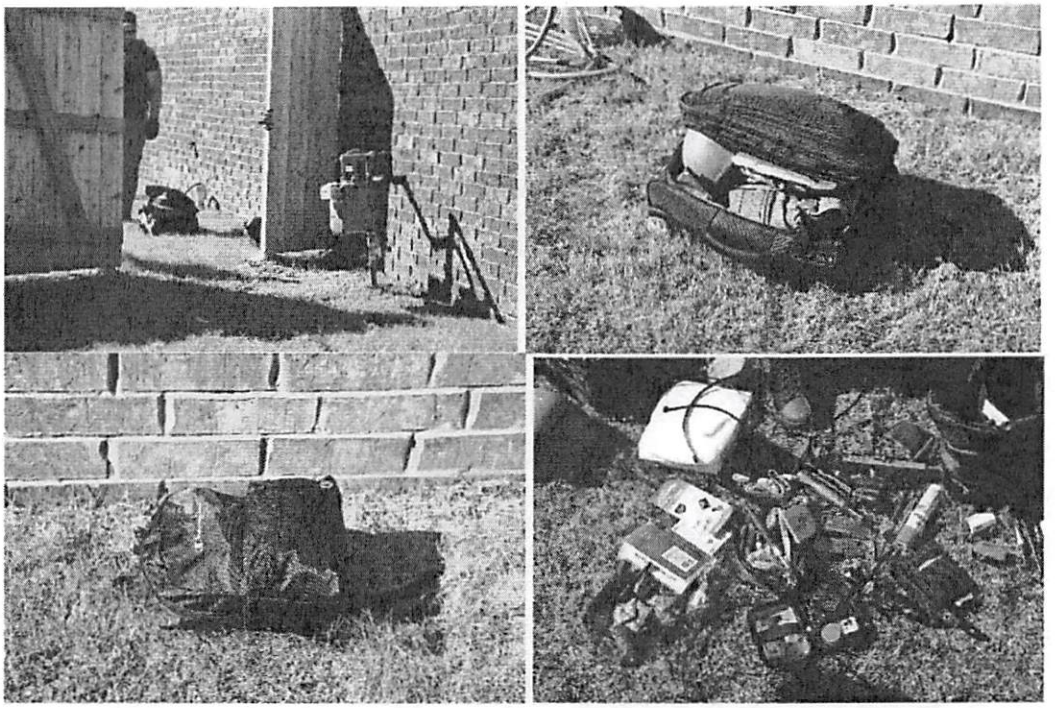
14. USMS Deputies and ATF Agents began retracing WINDSOR's steps. Supervisory Deputy John Gage observed two bags, a black Champion back-pack and a small suitcase, in the yard of the residence located at 3504 Easter 143rd Place South, Bixby, Oklahoma. This residence was adjacent to the residence from which WINDSOR was observed leaving. Mr. Zach Hammitt is the lessee of said address. Mr. Hammitt said that the bags in his yard did not belong to him. In fact, he said that the only reason he knew the bags existed was because an officer told him there were bags in his yard. (Mr. Hammitt provided the agents with a written affidavit to this fact.)

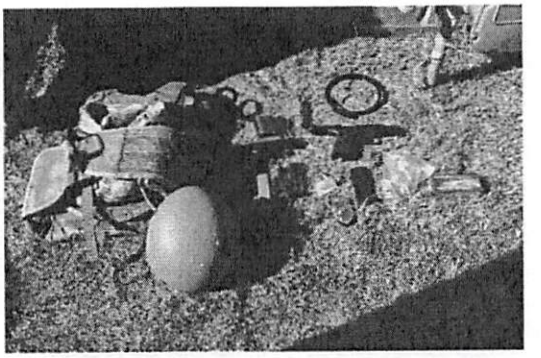
15. At this point, USMS Deputy Canine Handler Dayne Williams utilized his canine partner, Hudson who alerted to the presence of an explosive odor emanating from the bag. The bags were subsequently opened.

16. Inside the suitcase, agents located a Ruger Model 57, 5.7 x 28 semi-automatic pistol bearing serial number 641-04497. This firearm was loaded with 21 rounds of Fabrique Nationale Belgique 5.7 x 28 caliber ammunition. Also found inside the suitcase was a box containing 50 rounds of Remington 9mm Luger ammunition. A plastic baggy containing 19 rounds of assorted .40 caliber ammunition was found as well. A tan pistol magazine containing 18 rounds of assorted 9mm Luger ammunition was inside the suitcase. A smaller bag inside the suitcase was found and inside of this bag was a small plastic bag that contained a white crystalline substance which had an approximately gross weight of one (1) gram. The substance was suspected to be methamphetamine. The bag also contained a large amount of drug paraphernalia to include a set of electronic digital scales and numerous plastic baggies consistent with the distribution of controlled substances. The suitcase also contained a large camouflage Protective Products Body Armor bearing serial number PP0060134. Inside the pockets of the

body armor were a ski-mask, brass knuckles, gloves and zip-ties. (This is commonly known as a robbery kit.) The suitcase also contained a green Kevlar helmet. Handcuffs and a "Fugitive Task Force" badge were also found inside the suitcase.

17. Inside of the Champion backpack, agents found a loaded Smith and Wesson Model SW40VE .40 caliber semi-automatic pistol bearing serial number RBP5118. Two magazines containing 28 rounds of assorted. 40 caliber ammunition were also found in this bag. A smaller black case was found and inside of this case were several items of marijuana "dab" and marijuana oil/wax.





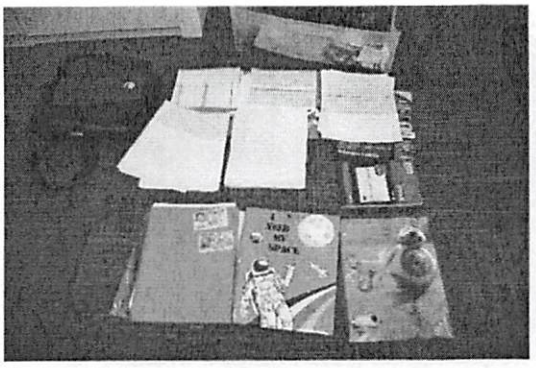
18. The residence, from which WINDSOR exited was being leased by SHARKEY. SHARKEY informed the agents that WINDSOR arrived on October 18th, 2020 and had a pistol in his possession. She described this pistol as potentially being a Smith and Wesson silver in color. He wore this firearm on his hip. When he arrived at her residence he brought suitcases and duffel bags with him. She saw the suitcase and black bag in the neighbor's yard and identified those bags as belonging to WINDSOR. SHARKEY also provided agents with consent to search her residence. SHARKEY signed the ATF Form 3220.11, Consent to Search.

19. In the master bedroom, under the mattress, agents found a loaded Glock Model 43X 9mm semi-automatic pistol bearing serial number BLTY279. Ten rounds, to include the round in the chamber, of Federal 9mm ammunition were in the magazine (and chamber loaded).

20. In the closet of the master bedroom, agents located a smaller black bag which contained four different plastic bags of marijuana which had an approximate gross weight of four (4), eight (8), seven (7) and seven (7) grams respectively. A black bottle was also found in this bag. Inside of the black bottle were a plastic baggy containing an approximate gross weight of 1 gram of a white powdery substance, a plastic baggy containing an approximate gross weight of 1 gram of an orange powdery substance and a plastic baggy containing an approximate gross weight of 5 grams of suspected marijuana. Also in the closet, agents found a fake coke can

utilized to secret objects. Inside the can, agents found a plastic baggy that contained five white pills.

21. In the closet agents found a Microsoft Surface Pro laptop bearing serial number 002181271557 (the Device), which SHARKEY alleged belonged to WINDSOR. A HP scanner, HP printer and a Canon printer, scanner and copier combination machine were also found. In the plastic shelf, on which the laptop and printers were sitting, agents found numerous pages of what appeared to be fraudulent blank checks and blank check forms. An envelope, which contained numerous checks addressed to other individuals and from different individuals was found. These checks appeared to have been stolen, as there was no indication or names that would connect to WINDSOR as being the rightful recipient of said financial documents. It should be noted that the earliest date observed on one of the stolen checks was dated September 25th, 2019.



22. In the living room of the residence, agents observed a television which was displaying the surveillance cameras that were affixed to the residence. Agents were provided the security code by SHARKEY. Agents were able to replay the day's earlier events and observed WINDSOR exiting the residence with the same bags that were found in the neighbor's yard.

23. The Device is currently in the lawful possession of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). It came into ATF's possession in the following way: as noted above, the Device was seized pursuant to a consensual search allowed by Ms. Sharkey of her residence. The Device was found to be in the master bedroom closet with other items associated with forgery and counterfeiting operations. Therefore, while ATF might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

24. The Device is currently in storage at ATF Tulsa Field Office Evidence Vault Exhibit 000022 located at 125 W 15th Suite 600, Tulsa, Oklahoma, within the Northern District of Oklahoma. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the ATF.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, and research, I know that the Device has capabilities to access the internet, has an IP Address. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

1. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

2. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

3. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the

attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

4. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

5. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

6. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Ashley N. Stephens
Senior Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

by phone

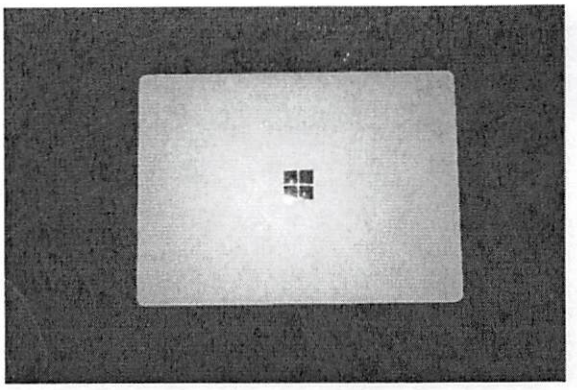
Subscribed and sworn to before me on November 16, 2020.

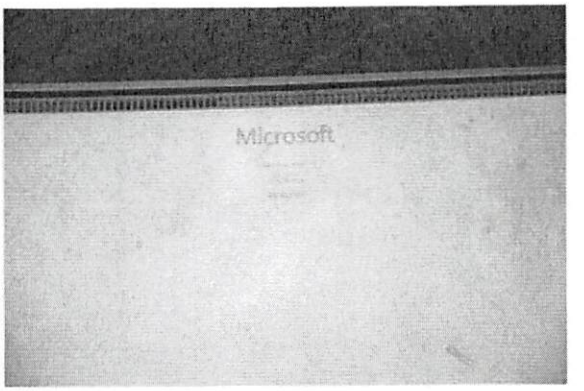
Frank H. McCarthy
UNITED STATES MAGISTRATE JUDGE

Paul J. Cleary
U.S. Magistrate Judge
333 W. 4th Street
Room 3355 U.S. Courthouse
Tulsa, OK 74103

ATTACHMENT A

The property to be searched is a Microsoft Surface Pro Laptop, serial number 002181271557 hereinafter the "Device." The Device is currently located inside the evidence vault of the Bureau of Alcohol, Tobacco Firearms and Explosives Tulsa Field Office located at 125 W 15th Suite 600, Tulsa within the Northern District of Oklahoma. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.





ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 USC 922(g)(1), 18 USC 922(g)(2), 21 USC 841(a)(1), 21 USC 846, 18 USC 1344, 18 USC 1028, 18 USC 1028A, 18 USC 513 and 18 USC 1344 including:

a. records relating to communication with others as to the criminal offense above; including incoming and outgoing voice messages; text messages; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;

b. records relating to documentation or memorialization of the criminal offense above, including voice memos, photographs, videos, and other audio and video media, and all ExIF information and metadata attached thereto including device information, geotagging information, and information of the relevant dates to the media;

c. records relating to the planning and execution of the criminal offense above, including Internet activity, including firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

d. application data relating to the criminal offense above;

e. lists of customers and related identifying information;

f. types, amounts, and prices of drug trafficked as well as dates, places, and amounts of specific transactions; and

g. any information related to sources of drugs and/or fraud related documents, securities, and checks, (including names, addresses, phone numbers, or any other identifying information);

h. any information recording WINDSOR's schedule or travel;

i. all bank records, checks, credit card bills, account information, and other financial records.

j. any fictitious identification cards, information or other items used for purpose of creating false documents

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. All records and information related to the geolocation of the Devices at a specific point in time; and

4. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the statutes listed in Paragraph 1 of this Attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.